John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JOSHUA OLUWALOWO, *on behalf of himself and all others similarly situated,*

Plaintiff,

v.

PANDA RESTAURANT GROUP, INC.; PANDA EXPRESS, INC.

Defendants.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Joshua Oluwalowo ("Plaintiff"), on behalf of himself and all others similarly situated ("Class Members"), files this Class Action Complaint ("Complaint") against Defendants Panda Restaurant Group, Inc. ("Panda Restaurant Group") and Panda Express, Inc. ("Panda Express") (collectively, "Defendants") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to safeguard and secure the personally identifiable information ("PII") of their current and former employees around the nation,[1] including Plaintiff. The individuals affected are former and current employees of Defendants and their affiliates, whose PII was maintained but insufficiently secured by Defendants.

2. The PII reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. As a result of Defendants' negligence, from approximately March 7, 2024 to March 11, 2024, cybercriminals were able to gain access to Defendants' corporate systems, which contain data records and sensitive and valuable PII (the "Data Breach"). On information and belief, information disclosed in the Data Breach includes but is not limited to names or other personal identifiers, dates of birth, social security numbers, driver's license numbers, and non-driver identification card numbers.[2]

---

[1] *Panda Express Is The Latest To Be Hacked. What To Do When Your Personal Data Are Exposed*, LOS ANGELES TIMES (May 2, 2024), https://www.latimes.com/california/story/2024-05-02/panda-kaiser-att-data-breaches-how-to-protect-yourself.

[2] *See* Letter sent by Panda Express to Plaintiff, Notice of Data Security Incident (Apr. 30, 2024) (attached as Exhibit 1) ("Notice Letter"); Sergiu Gatlan, *Panda Restaurants discloses data breach after corporate systems hack*, BLEEPINGCOMPUTER (May 1, 2024), https://www.bleepingcomputer.com/news/security/panda-restaurants-discloses-a-data-breach-after-corporate-systems-hack/.

3. Defendant Panda Express is the largest Chinese fast food chain in the United States, with over $3 billion in sales and 47,000 associates working in over 2,300 branches.[3]

4. Defendant Panda Restaurant Group is the parent company of Panda Inn, Panda Express, and Hibachi-San.[4] Defendants and their affiliates jointly operate their restaurants in 43 states throughout the nation.[5]

5. The total number of individuals whose PII was exposed due to Data Breach is unknown at this time but is estimated to be in the tens of thousands.

6. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial information in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, and using Class members' PII to target other phishing and hacking intrusions.

7. Defendants owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and

---

[3] Gatlan, *supra* n.2.

[4] *See About Us*, PANDA RESTAURANT GROUP, INC., https://www.pandarg.com/about-us.html (last visited May 10, 2024).

[5] *Id.*

maintain reasonable security procedures and practices to protect their current and former employees' PII from unauthorized access and disclosure.

8. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiff and Class members as a result. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach.

9. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of financial fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

10. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendants' data security system, future annual audits, and adequate credit monitoring services funded by Defendants.

11. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, and breach of implied contract, and seeks declaratory relief, injunctive relief, monetary damages,

statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

12. Plaintiff Joshua Oluwalowo resides in Hennepin County, Minnesota. Mr. Oluwalowo was an employee of Panda Express and provided his PII to Defendants as a condition of his employment.

13. On or around April 30, 2024, Mr. Oluwalowo received a notice notifying him of the Data Breach and that his name, social security number, and date of birth were exposed due to the Data Breach ("Notice Letter").[6]

14. After the Data Breach, Plaintiff has been forced to spend time and money addressing and attempting to mitigate further harm and injury resulting from the Data Breach. Plaintiff has spent substantial time changing all his passwords to other accounts, several of which (including his personal email account) have been subject to unauthorized, attempted logins from international locations. Plaintiff has also suffered emotionally over the stress resulting from the Data Breach and his substantially increased risk of identity theft.

15. Had Plaintiff known that Defendants would not adequately protect his and Class members' PII, he would not have entered into an employment relationship

[6] *See* Notice Letter, *supra* n.2.

with Defendants or any of their affiliates and would not have provided his PII to Defendants or any of their affiliates.

16. At all relevant times, Plaintiff is and continues to be a member of the Class.

17. Defendant Panda Restaurant Group is a limited liability corporation that maintains its headquarters at 1683 Walnut Grove Avenue, Rosemead, California 91770.

18. Defendant Panda Express is a stock corporation that maintains its headquarters at 1683 Walnut Grove Avenue, Rosemead, California 91770.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

20. This Court has general personal jurisdiction over Defendants because Defendants are citizens of California. Moreover, Defendants have sufficient minimum contacts in the State, and Defendants engaged in the conduct underlying this action in California, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class members' PII. Defendants intentionally

availed themselves of this jurisdiction by marketing and selling products and services and accepting and processing payments for those products and services within the State.

21. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendants do business in this Judicial District.

FACTUAL ALLEGATIONS

Overview of Defendants

22. Defendants Panda Restaurant Group and its affiliates operate the largest Chinese fast food chain in the United States, Defendants Panda Express, with over 47,000 associates working in over 2,300 restaurants in 43 states throughout the nation.[7]

23. Plaintiff and Class members are current and former employees of Defendants.

24. To obtain an employment relationship with Defendants, employees like Plaintiff and Class members are required to, and did, provide Defendants directly with sensitive PII.

25. In the regular course of their business, Defendants collect, store, and maintain the PII they receive from employees who utilize Defendants' products and or/services.

[7] Gatlan, *supra* n.2.

26. By creating and maintaining massive repositories of PII, Defendants have provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

The Data Breach and Notice Letter

27. Between approximately March 7, 2024, and March 11, 2024, the PII of current and former employees were leaked due to an external system breach.[8]

28. Specifically, on approximately March 10, 2024, Defendants detected the Data Breach.[9] After an internal investigation, Defendants determined that certain information on their corporate systems was exposed between March 7 and March 11, 2024.[10]

29. On April 15, 2024, after their review of impacted data, Defendants confirmed that their employees' PII, including but not limited to, includes but is not limited to names or other personal identifiers, dates of birth, social security numbers, driver's license numbers, and non-driver identification card numbers.[11]

30. While Defendants claim in their Notice Letter that they "took immediate action to secure our environment, activated [its] remediation and

---

[8] *See Data Breach Entry*, OFF. OF MAINE ATT.'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/7ca9584e-dc2d-4fae-b48b-1580700e1afc.shtml (last visited May 12, 2024) (data breach report submitted by Defendant); Notice Letter, *supra* n.2.

[9] Notice Letter, *supra* n.2.

[10] *Id.*

[11] *Id;* Gatlan, *supra* n.2.

recovery efforts, and launched a thorough investigation in partnership with third-party cybersecurity specialists to determine the nature and scope of the incident[,]" Defendants fail to further specify those purported actions or efforts.[12]

31. Defendants waited over a month from the date they learned of the Data Breach to notify the affected individuals.

32. To date, Defendants have not disclosed crucial information, including, but not limited to, the identity of the hacking group responsible for the Data Breach, how the cybercriminals were able to exploit vulnerabilities in Defendants' IT security systems, or any specific steps taken by Defendants to safeguard their systems.

33. Defendants did not use reasonable security procedures to safeguard the sensitive information of Plaintiff and Class Members.

34. Defendants' systems hacked by cybercriminals contained Plaintiff's and Class members' PII that was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

35. Plaintiff and Class members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligation to keep such information confidential and secure from unauthorized access.

---

[12] *Id.*

36. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendants assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

Defendants Knew That Criminals Target PII.

37. At all relevant times, Defendants knew or should have known that Plaintiff's and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

38. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

39. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[13]

[13] *See, e.g., Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited May 10, 2024).

40. As a result of the notoriety of cyberattacks on systems like Defendants', several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

41. In light of the high-profile data breaches in similar industries and large businesses, and a wealth of relevant guidance and news reports at Defendants' disposal, Defendants knew or should have known that cybercriminals would target their electronic records and employees' PII.

42. These data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to improve the security of their systems and engage in stronger, more comprehensive cybersecurity practices.

43. PII is a valuable property right.[14] The value of PII as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated

---

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[15] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-

to have spent over $19 billion acquiring consumers' personal data in 2018.[17] In fact, PII is so valuable to identity thieves that once disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

44. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, and other PII directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

45. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[18]

---

technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[18] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

46. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

47. Therefore, Defendants clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII stored in their unprotected files and the massive amount of PII they maintain.

Theft of PII has Grave and Lasting Consequences for Victims.

48. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[19]

[19] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

49. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[20] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[21]

50. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

51. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[22] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes

---

[20] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[21] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited May 12, 2024).

[22] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

time for the victim to become aware of the theft, and the theft can adversely impact the victim's credit rating.

52. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[23]

53. There may be a time lag between when PII is stolen and when it is used.[24] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

54. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade it on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers,

---

[23] *Id.* at 2, 9.

[24] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[25] U.S. GOV'T ACCOUNTABILITY OFF., *supra* n.22 at 29 (emphasis added).

Social Security Numbers, and other PII directly on various Internet websites, making the information publicly available.

55. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who companies employ to find flaws in their computer systems, stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[26]

56. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[27]

57. Plaintiff and Class members must vigilantly monitor their financial accounts and their family members' accounts for many years to come.

58. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by

---

[26] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[27] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://efraudprevention.com/pub/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited May 12, 2024).

people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

59. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (v) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

60. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

61. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All of Defendants' current and former employees whose PII was accessed by unauthorized persons as a result of the Data Breach between March 7, 2024 and March 11, 2024.

62. Plaintiff reserves the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

63. Plaintiff is a member of the Class.

64. Excluded from the Class are Defendants, their affiliates, parents, subsidiaries, officers, agents, directors, the judge(s) presiding over this matter, and the clerks of said judge(s).

65. This action seeks both injunctive relief and damages.

66. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

67. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of Class members is unknown at this time, Class members are readily identifiable in Defendants' records, which will be a subject of discovery. Upon information and belief, there are tens of thousands of Class members in the Class.

68. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;
c. Whether Defendants owed a duty to Plaintiff and Class members to safeguard their PII;
d. Whether Defendants breached their duty to Plaintiff and Class members to safeguard their PII;
e. Whether Defendants failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class members;
f. Whether Plaintiff's and Class members' PII was compromised in the Data Breach;
g. Whether Plaintiff and Class members are entitled to injunctive relief; and
h. Whether Plaintiff and Class members are entitled to damages as a result of Defendants' conduct.

69. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and violations of law. Plaintiff and Class members all had their PII stolen in the Data Breach. Plaintiff's grievances, like the proposed Class members' grievances, all arise out of the same business practices and course of conduct by Panda Express.

70. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

71. Plaintiff and his chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") and Milberg Coleman Bryson Phillips Grossman, PLLC (collectively, "Plaintiff's Counsel") -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this

Complaint. In particular, FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. Plaintiff's Counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class members. Finally, Plaintiff's Counsel possess the financial resources necessary to ensure that a lack of financial capacity will not hamper the litigation and is willing to absorb the costs of the litigation.

72. **Predominance.** The common issues identified above arising from Defendants' conduct predominate over any issues affecting only individual Class members. The common issues hinge on Defendants' common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

73. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive

cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

74. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendants has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class members, in terms of monetary damages due and terms of equitable relief, can be determined in this single proceeding rather than in multiple individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief to the Class members and Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only current and former employees of Defendants, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice

procedures unworkable or overly expensive. The identity of the Class members can be identified from Defendants' records, such that direct notice to the Class members would be appropriate.

75. **Injunctive relief.** Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

76. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

77. As a condition of engaging in employment with Defendants, Plaintiff and Class members were required to and did provide Defendants with their PII.

78. By collecting and storing their PII, at all times relevant, Defendants owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in their possession, custody, or control.

79. Defendants owed a duty of care to Plaintiff and Class members to provide data security consistent with statutory and industry standards and to ensure that their systems and networks and the personnel responsible for them adequately protected the PII.

80. Defendants knew the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems.

Defendants knew of the many data breaches that targeted companies that store PII in recent years.

81. Given the nature of Defendants' businesses, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

82. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them -- including Plaintiff's and Class members' PII.

83. Plaintiff and Class members are a well-defined, foreseeable, and probable group of employees that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

84. Plaintiff and Class members have no ability to protect their PII that was or remains in Defendants' possession.

85. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor,

and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

86. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

87. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiff's and Class members' PII and failing to provide them with timely notice that their PII had been compromised.

88. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

89. By failing to provide timely and complete notification of the Data Breach to Plaintiff and Class members, Defendants prevented them from proactively taking steps to secure their PII and mitigate the associated threats.

90. As a result of Defendants' above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, inter alia: (i) a

substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

91. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

92. Defendants had duties by statute to ensure that all information they collected and stored was secure and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class members' PII.

93. Defendants' duties arise from, *inter alia*, Section 5 of the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45(a)(1) ("FTCA"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

94. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[28]

95. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendants must take to meet their data security obligations and effectively put Defendants on notice of these standards.

96. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all Class members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable

[28] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

given the nature and amount of PII they obtain and store, and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiff and other Class members.

97. Defendants' violation of the FTCA constitutes negligence per se.

98. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

99. The harm occurring as a result of the Data Breach is the type of harm against which Section 5 of the FTCA was intended to guard.

100. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

101. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violation of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for

protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

102. Defendants' violation of the FTCA constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

103. Defendants owed a duty of care to Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

104. It was foreseeable that Defendants' failure to use reasonable measures to protect PII and provide timely notice of the Data Breach would result in injury to Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

105. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF FIDUCIARY DUTY

106. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

107. Plaintiff and Class members gave Defendants their PII in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Defendants and Plaintiff and Class members.

108. In light of this relationship, Defendants have a fiduciary duty to act primarily for the benefit of Plaintiff and Class members upon matters within the scope of their relationship, which includes safeguarding and protecting Plaintiff's and Class members' PII.

109. Defendants breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII and otherwise failing to safeguard Plaintiff's and Class members' PII that they collected.

110. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (v) the continued risk to their PII which remains in Defendants' possession; and (vi) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

111. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

112. As a condition of their employment with Defendants, Plaintiff and all other Class members provided their PII to Defendants and entered into implied contracts with Defendant.

113. Pursuant to these implied contracts, in exchange for the consideration and PII provided by Plaintiff and Class members, Defendants agreed to, among other things, and Plaintiff understood that Defendants would: (1) enter into employment relationships with Plaintiff and Class members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

114. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other.

115. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their PII and paid for the services from Defendant.

116. Plaintiff and Class members would not have entrusted their PII to Defendants in the absence of such an implied contract.

117. Defendants breached their obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

118. Defendants' breach of their obligations under their implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered.

119. Defendants' breach of implied contracts injured Plaintiff and all other Class members because (i) they provided their PII to Defendants as a condition of their employment, and performed services for Defendants' benefit, with the expectation of data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred, and future costs required, to mitigate and

remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in his favor and against Defendants as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiff as Class representatives and the undersigned counsel as Class Counsel;

B. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 15, 2024

Respectfully submitted,

By: /s/ *John J. Nelson*

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
Todd S. Garber
Pro hac vice forthcoming
Andrew C. White
Pro hac vice forthcoming
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Attorneys for Plaintiff and the Proposed Class